भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

राज्य सभा

अतारांकित प्रश्न संख्या 706

जिसका उत्तर 05 दिसंबर, 2025 को दिया जाना है ।

14 अग्रहायण, 1947 (शक)

सरकारी अधिकारियों द्वारा एआई प्लेटफॉर्म के बढ़ते उपयोग के कारण डेटा लीक का खतरा

706. श्री एस. निरंजन रेड्डी:

क्या इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री यह बताने की कृपा करेंगे कि:

(क) क्या सरकार को इस बात की जानकारी है कि जब सरकारी अधिकारी नोट बनाने, विश्लेषण या प्रशासनिक सहायता के लिए जनरेटिव एआई प्लेटफॉर्म का उपयोग करते हैं, तो उन टूल्स में डाले गए प्रॉम्प्ट से संवेदनशील जानकारी लीक होने का खतरा हो सकता है;

(ख) क्या एआई प्रणालियों द्वारा सरकारी नीतियों से संबंधित इनपुट को संग्रहीत करने, प्रोफाइलिंग करने या उनसे सीखने के जोखिम का कोई आकलन किया गया है;

(ग) क्या सिविल सेवकों द्वारा वाणिज्यिक एआई उपकरणों के उपयोग को विनियमित करने के लिए दिशानिर्देश जारी किए गए हैं या प्रस्तावित हैं;

(घ) क्या सरकार आधिकारिक उपयोग के लिए सुरक्षित संप्रभु एआई मॉडल या इन-हाउस लार्ज लैंग्वेज मॉडल (एलएलएम) स्थापित करने का प्रस्ताव रखती है; और

(ङ) यदि हाँ, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से (ड.): भारत की एआई रणनीति प्रौद्योगिकी के लोकतंत्रीकरण के माननीय प्रधानमंत्री के दृष्टिकोण पर आधारित है। इसका उद्देश्य भारत केंद्रित चुनौतियों का समाधान करना और अवसर तैयार करना है।

सरकार सरकारी अधिकारियों द्वारा जनरेटिव एआई के उपयोग से जुड़े जोखिमों से अवगत है। किसी भी एआई उपकरण या आईटी उत्पादों का उपयोग करने वाले सरकारी अधिकारी, आधिकारिक गोपनीयता अधिनियम के प्रावधानों के अधीन हैं और उनसे उन प्लेटफार्मों पर किसी भी वर्गीकृत या संवेदनशील जानकारी को साझा करने की अपेक्षा नहीं की जाती है जो सुरक्षित नहीं हैं या भारत के बाहर होस्ट किए गए हैं।

ओपन-सोर्स मॉडल की होस्टिंग: एआई उपकरणों तक सुरक्षित पहुंच को बढ़ावा देने के लिए, एमईआईटीवाई ने सी-डैक पुणे द्वारा प्रबंधित ऐरावत कंप्यूट इंफ्रास्ट्रक्चर पर ओपन-सोर्स एआई मॉडल की होस्टिंग को सक्षम किया है। यह संवेदनशील डेटा को देश से बाहर स्थानांतरित करने के जोखिम को समाप्त करता है। एलएलएएमए, ओपन एआई और मिस्ट्रल फैमिलीज़ के मॉडल नियोजित किए गए हैं। इन्हें प्रभार्य आधार पर एपीआई के माध्यम से डेवलपर्स को भी उपलब्ध कराया जा रहा है।

इसके अलावा, एनआईसी सरकारी उपयोगकर्ताओं के लिए एनआईसी के मेघराज क्लाउड के माध्यम से परिसर में स्थापित ओपन-सोर्स मॉडल तक पहुंच प्रदान कर रहा है।

एआईकोश प्लेटफॉर्म के तहत, भारत के लिए विशिष्ट 251 एआई मॉडल और 27 से अधिक विकास टूलकिट भी उपलब्ध कराए गए हैं।

इंडियाएआई मिशन के तहत भारत के अपने मूलभूत मॉडल: सरकार ने मार्च 2024 में इंडियाएआई मिशन लॉन्च किया। इंडियाएआई फाउंडेशन मॉडल स्तंभ का उद्देश्य जनरेटिव एआई में संप्रभु क्षमता और वैश्विक प्रतिस्पर्धा सुनिश्चित करने के लिए भारतीय डेटासेट और भाषाओं पर प्रशिक्षित भारत के अपने बड़े मल्टीमॉडल मॉडल विकसित करना है।

सर्वम एआई, सोकेट एआई, ज्ञानी एआई, गण एआई, अवतार एआई, आईआईटी बॉम्बे कंसोर्टियम (भारतजेन), जेनलूप, जेंटीक, इंटेलीहेल्थ, शोध एआई, फ्रैक्टल एनालिटिक्स लिमिटेड और टेक महिंद्रा मेकर लैब सहित स्टार्टअप, उद्योग प्लेयर्स और शैक्षणिक संस्थानों सहित **बारह संगठनों और कंसोर्टिया** को भारतीय डेटासेट के आधार पर बड़े और छोटे भाषा मॉडल विकसित करने के लिए चुना गया है।

परिणामी एआई मॉडल ओपन-सोर्स इकोसिस्टम में योगदान देंगे और सरकारी संगठनों द्वारा उपयोग के लिए उपलब्ध होंगे और भारत के स्टार्टअप और अनुसंधान समुदाय में नवाचार का भी समर्थन करेंगे।

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन): भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) द्वारा जारी दिशानिर्देशों में एआई उपकरणों के सुरक्षित और जिम्मेदार उपयोग के लिए विशिष्ट सुरक्षा उपाय प्रदान किए गए हैं:

- आर्टिफिशियल इंटेलिजेंस (एआई) आधारित अनुप्रयोगों से उत्पन्न होने वाले प्रतिकूल खतरों को कम करने के लिए किए जाने वाले सुरक्षा उपायों पर परामर्शी निदेश मई 2023 में प्रकाशित किए गए थे।
- सर्टिफाइड सिक्योरिटी प्रोफेशनल इन आर्टिफिशियल इंटेलिजेंस (सीएसपीएआई) कार्यक्रम सितंबर, 2024 में सर्ट-इन और एसआईएसए द्वारा लॉन्च किया गया।
- जनरेटिव एआई समाधानों के प्रभावी और जिम्मेदार उपयोग के लिए श्रेष्ठ पद्धतियों को दर्शाने वाला एक परामर्शी निदेश मार्च 2025 में प्रकाशित किया गया था।
- सीएसपीएआई कार्यक्रम साइबर सुरक्षा पेशेवरों को एआई सिस्टम को सुरक्षित करने, एआई से संबंधित खतरों को सक्रिय रूप से कम करने और व्यावसायिक वातावरण में भरोसेमंद एआई परिनियोजन सुनिश्चित करने के कौशल से लैस करता है।
- सर्ट-इन ने एएनएसएसआई की फरवरी 2025 की रिपोर्ट "साइबर-जोखिम-आधारित दृष्टिकोण के माध्यम से एआई में विश्वास का निर्माण" पर सह-हस्ताक्षर किए, जिसमें एआई सिस्टम और मूल्य श्रृंखलाओं को सुरक्षित करने के लिए जोखिम-आधारित ढांचे की वकालत की गई और विश्वसनीय विकास के लिए एआई से संबंधित साइबर जोखिमों को कम करने पर वैश्विक संवाद का आग्रह किया गया।

*****